Elementos de Criptografia

LMAC, LEIC, MEIC

Exame 2 - 16 val.

Duração: 3 horas

Grupo I 1.0+1.0+1.0

1 Demonstre o Teorema de Shannon. Prove ou encontre um contra-exemplo para a seguinte asserção: Se $\mathcal{T}$ e $\mathcal{T}'$ são incondicionalmente seguros então $\mathcal{T} \circ \mathcal{T}'$ é incondicionalmente seguro.

2 Mostre como é que o fluxo por blocos da cifra de Hill pode ser representada como um fluxo de chaves da cifra de Viginère.

3 Descreva sucintamente o algoritmo de cifração do DES e como este pode ser utilizado em blocos.

Grupo II 2.5+2.5

1. Apresente a correcção do sistema criptográfico de ElGamal. Mostre como pode atacar este sistema para Z_p quando $p - 1 = 2^n$.

2. Considere o sistema criptográfico RSA sobre Z_n com $n = p \times q$ e seja $f : RQ(n) \to Z_n$ um mapa que transforma um resíduo quadrático y numa raíz não trivial deste. Considere a seguinte linguagem $L \subseteq Z_n \times RQ(p)$ tal que $L(x, y) = 1$ sse $x < f(y)$. Mostre que se $L \in \mathbf{P}$ então é possível analisar em tempo polinomial o sistema criptográfico RSA, apresentado a análise de complexidade do seu algoritmo.

Grupo III 1.5+2.5

1. Descreva o sistema de partilha de segredo de Shamir baseado na interpolação de polinómios. Desenvolva uma variante para resolver o seguinte problema, um grupo de 3 generais e 3 políticos deseja partilhar uma chave de tal modo que: (1) seja necessário a coligação de 3 elementos para gerar a chave secreta; (ii) nesta coligação deve existir pelo menos 1 político e 1 general.

2. Considere o seguinte sistema de prova de conhecimento nulo baseado em resíduos quadráticos. A Alice diz possuir uma raíz quadrada de x em Z_n com $n = pq$, p, q primos. (i) No primeiro passo a Alice gera o resíduo quadrático $y = v^2 \mod n$ e envia y ao Bruno. (ii) O Bruno gera aleatoriamente $r \in \{0, 1\}$ e envia r à Alice. (iii) A Alice envia $z = u^r v$ ao Bruno. (iv) Finalmente, o Bruno verifica se $z^2 = x^r y$. Caso a condição (iv) se verifique itera estes passos $\log(n)$ vezes, e se a condição (iv) se verificar em todas estas iteradas acredita que a Alice possui uma raíz de x. Prove que este protocolo é correcto, adequado e é de conhecimento nulo.

Suponha que a Alice deseja que o Bruno se comprometa com um bit b numa certa data t. Esse bit deverá ser conhecido apenas pelo Bruno até que um certo evento aconteça na data $t + k$. Nesta altura o Bruno deverá demonstrar à Alice que se tinha comprometido com b, devendo ser impossível (em tempo polinomial) a Bruno conseguir demonstrar que se tinha comprometido com $1 - b$. Apresente um protocolo para resolver este problema.